Cassandra Crossing/ Privacy e olio di serpente

(9)—C'è chi si fida dei sistemi operativi chiusi, spesso non ha alternative, ma come fa quella stessa persona a fidarsi anche di sistemi…

Cassandra Crossing/ Privacy e olio di serpente

Figure 1:

(9)—C'è chi si fida dei sistemi operativi chiusi, spesso non ha alternative, ma come fa quella stessa persona a fidarsi anche di sistemi crittografici che non siano open source?.

28 ottobre 2005—Man mano che l'uso di strumenti per la privacy si diffonde (sempre troppo lentamente per i miei gusti) mi rendo conto che i problemi che devono essere affrontati da tutti aumentano di numero. Facciamo un esempio banale: i programmi closed source.

Voi comprereste un medicinale senza nome, da uno sconosciuto incontrato per la strada, perché vi ha detto che èun ricostituente e vi farà sentire meglio? Ovviamente no.

E comprereste un programma per la privacy, ad esempio un programma per crittografare la posta, da una qualunque software house commerciale che non vi metta a disposizione i sorgenti ma vi assicuri che è inattaccabile e sicurissimo? La risposta, specialmente nel caso dei programmi per la privacy, è di nuovo "*Ovviamente no*".

Cosa mi garantisce che il programma non sia privo di errori o, peggio, addirittura compromesso volontariamente ?

E' il motivo per cui i programmi per la privacy devono avere il codice sorgente aperto ed anche una documentazione degli algoritmi che usano. "*Ma—si dirà—se ritenessi necessario questo,*

allora dovrei poter avere i sorgenti del sistema operativo che uso e di tutte le applicazioni, e controllarmelo tutto. Impossibile!"

Bene, cominciamo a dire che la possibilità di avere i sorgenti di tutto il proprio ambiente operativo, dai driver alla applicazioni, esiste. Basta utilizzare GNU/Linux od altri sistemi operativi ed applicazioni a sorgente aperto.

Ma anche se per scelta o per vincolo si utilizzassero sistema operativo ed applicazioni a sorgente chiuso, come Windows ed Outlook, e quindi si diminuisse la verificabilità del proprio ambiente operativo, la si perderebbe completamente utilizzando software crittografico, di firma elettronica o comunque destinato alla salvaguardia della privacy, a sorgente chiuso.

E' in questi software infatti, che si trova la vostra prima linea di difesa della privacy.

Datemi pure del paranoico. Oltre alla solita risposta che "*la paranoia è una virtù*'" passo a fare un paio di esempi.

Ben due (tra quelle a me note) software house commerciali che vendono programmi per la cancellazione sicura dei dischi si vantano di utilizzare **l'algoritmo di Gutmann a 35 passate**.

Bene, questo algoritmo è legato all'hardware dei dischi rigidi, ed in particolare ai dischi con codifica RLL; non facciamola troppo lunga, sono i dischi dei pc della generazione 8086/80286; quelli di oggi sono completamente diversi e l'algoritmo di Gutmann non ha nessuna particolare efficacia.

Solo olio di serpente, insomma. E se non avessero documentato l'algoritmo come sarebbe stato possibile accorgersene? ("Secure Deletion of Data…"—Peter Gutmann, VI USENIX conference, 1996).

Nel novembre del 2003, durante un controllo di routine del software del kernel 2.6 di Linux (allora in fase di rilascio) fu scoperta **una backdoor nei sorgenti del kernel**, ottenuta inserendo un singolo carattere (per la precisione un "=") in una singola riga. Non ci interessa qui dire da chi o per cosa, e nemmeno se altre modifiche del genere siano passate inosservate.

Il punto è che in nessun ambiente commerciale i sorgenti nel loro complesso sono visibili, e la probabilità che una modifica maliziosa del codice venga rivelata è senz'altro interi ordini di grandezza più bassa.

Allora, per finire questa digressione con una raccomandazione, quando crittografate od altro, fatelo con software a sorgente aperto. Una piccola fatica in più sarà un ottimo investimento in sicurezza. C'è molta più gente desiderosa di compromettere questi programmi di quanto non si pensi, e di sicuro è più di quella che vuole compromettere un sistema operativo.

E quando leggerete di programmi mirabolanti e supersicuri, che pero', poffarbacco, sono a sorgente chiuso e nemmeno documentati, statene lontani come dalla peste. Anche se ve li raccomandasse qualcuno di fiducia: tutti possono sbagliare.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on June 10, 2022.

Canonical link

Exported from Medium on August 27, 2025.